So vermeiden Sie Sicherheitsrisiken öffentlicher WLANs

https://www.kaspersky.de/resource-center/preemptive-safety/public-wifi-risks

WLAN-Benutzer sind Risiken durch Hacker ausgesetzt, doch glücklicherweise gibt es Möglichkeiten, sich zu schützen. Die starke Verbreitung kostenloser öffentlicher WLANs ist ein wahrer Segen für Berufstätige, die viel unterwegs sind. Da viele Restaurants, Hotels, Flughäfen, Buchhandlungen und sogar einige Einzelhandelsgeschäfte den freien Internetzugriff anbieten, erhalten Sie praktisch von überall aus Zugang zu Ihrem Netzwerk und Ihrer Arbeit. Diese Freiheit hat jedoch ihren Preis, und nur die wenigsten sind sich der Risiken öffentlicher WLANs wirklich bewusst. Nur wenn Sie lernen, wie Sie sich schützen, können Sie dafür Sorge tragen, dass wichtige Geschäftsdaten sicher bleiben.

Die Risiken öffentlicher WLANs

Dieselbe Eigenschaft, die kostenlose WLAN-Hotspots für die breite Öffentlichkeit so interessant macht, macht sie gleichzeitig auch so attraktiv für Hacker: Es ist keine Authentifizierung erforderlich, um eine Verbindung zum Netzwerk herzustellen. Hierdurch erhalten Hacker nämlich nahezu uneingeschränkten Zugriff auf ungesicherte Geräte im selben Netzwerk.

Die größte Sicherheitsbedrohung in frei zugänglichen WLANs ist die Möglichkeit für Hacker, sich zwischen Ihr Gerät und den Zugriffspunkt zu schalten. Anstatt also direkt mit dem Hotspot zu kommunizieren, senden Sie Ihre Daten zunächst an den Hacker, der sie dann weiterleitet.

Auf diese Weise hat der Hacker Zugriff auf alle Informationen, die Sie über das Internet übermitteln: vertrauliche E-Mails, Kreditkartendaten oder die Zugangsdaten für Ihr Unternehmensnetzwerk. Besitzt er diese Informationen erst einmal, kann der Hacker nach Belieben genau wie Sie auf Ihre Systeme zugreifen.

Hacker nutzen ungesicherte WLAN-Verbindungen darüber hinaus auch zur Verbreitung von Malware. Wenn Sie über ein Netzwerk Dateien austauschen, ist es für Profis ein Leichtes, infizierte Software auf Ihrem Computer einzuschleusen. Einigen findigen Hackern gelingt es sogar, den Zugriffspunkt selbst zu infiltrieren. Sie lassen dann während des Verbindungsaufbaus ein Popup-Fenster anzeigen, in dem Ihnen ein Upgrade für eine beliebte Software angeboten wird. Ein Klick auf dieses Fenster genügt bereits, um die Schadsoftware zu installieren.

Mit der zunehmenden Beliebtheit der mobilen WLAN-Nutzung kann man davon ausgehen, dass es langfristig immer häufiger zu Problemen mit der Internetsicherheit und zu einer Zunahme der Risiken in öffentlichen WLANs kommen wird. Das heißt jedoch nicht, dass kostenlose WLANs grundsätzlich tabu sind. Da die überwältigende Mehrheit der Cyberkriminellen auf leichte Beute aus ist, sollten einige wenige Sicherheitsvorkehrungen ausreichen, um Ihre vertraulichen Informationen zu schützen.

Nutzen Sie ein VPN

Eine virtuelle private Netzwerkverbindung (VPN) ist unverzichtbar, wenn Sie sich über eine ungesicherte Verbindung, wie z. B. einen WLAN-Hotspot, mit Ihrem Unternehmensnetzwerk verbinden. Selbst wenn es einem Hacker gelingen sollte, Ihre Verbindung abzufangen, werden die Daten bei einem VPN hochsicher verschlüsselt. Und da die meisten Hacker auf leichte Beute aus sind, werden sie sich kaum die Mühe machen zu versuchen, Ihre Daten aufwändig zu entschlüsseln.

Nutzen Sie SSL-Verbindungen

Wahrscheinlich haben Sie für die allgemeine Nutzung des Internets keine VPN-Verbindung verfügbar. Sie können Ihre Kommunikation aber trotzdem verschlüsseln. Aktivieren Sie auf Webseiten, die Sie oft besuchen oder bei denen Sie Zugangsdaten eingeben müssen, die Option „Immer HTTPS verwenden“. Vergessen Sie nicht, dass Hacker die Gewohnheiten des durchschnittlichen Benutzers bei der Verwendung von Zugangsdaten kennen und wissen, dass viele Benutzer für irgendein Forum und für Ihr Online-Banking und Ihr Unternehmensnetzwerk ein und dasselbe Passwort verwenden. Wenn Sie diese Anmeldeinformationen unverschlüsselt übermitteln, könnten Sie gerissenen Hackern Tür und Tor öffnen. Bei vielen Webseiten, für die ein Konto mit Anmeldeinformationen erforderlich ist, finden Sie die „HTTPS“-Option in den Einstellungen.

Deaktivieren Sie die Dateifreigabe

Wenn Sie sich über eine öffentliche Verbindung mit dem Internet verbinden, möchten Sie wahrscheinlich keine Ihrer Daten für andere freigeben. Sie können die Dateifreigabe je nach verwendetem Betriebssystem über die Systemeinstellungen bzw. die Systemsteuerung deaktivieren oder dies Windows überlassen, indem Sie die Option „Öffentlich“ wählen, wenn Sie sich zum ersten Mal mit einem neuen, ungesicherten Netzwerk verbinden.

Deaktivieren Sie WLAN, wenn Sie es nicht benötigen

Auch wenn Sie selbst keine Verbindung mit einem Netzwerk hergestellt haben, tauscht die WLAN-Hardware in Ihrem Gerät trotzdem Daten mit allen Netzwerken innerhalb der Reichweite aus. Es gibt Sicherheitsvorkehrungen, die verhindern, dass diese minimale Kommunikation zur Gefahr für Sie wird, aber nicht alle Wi-Fi-Router sind gleich aufgebaut und Hacker sind bekannt dafür, äußerst gerissen vorzugehen. Wenn Sie auf Ihrem Computer lediglich an einem Word- oder Excel-Dokument arbeiten, sollten Sie WLAN deaktivieren. Das beschert Ihnen zusätzlich eine längere Akkulaufzeit.

Sorgen Sie für dauerhaften Schutz

Auch wenn Sie alle nur erdenklichen Sicherheitsmaßnahmen für öffentliche WLANs ergreifen, können Sie nicht alle Risiken vollständig eliminieren. Dies lässt sich in unserer vernetzten Welt einfach nicht ausschließen. Aus diesem Grund sollten Sie ein zuverlässiges Internetsicherheitspaket auf Ihrem Computer installieren. Die Software überprüft alle Ihre Dateien laufend auf Schadsoftware – auch neue Dateien, die

gerade heruntergeladen werden. Hochwertige Sicherheitssoftware für Privatanwender enthält darüber hinaus auch Sicherheitsfunktionen zum Schutz Ihres Unternehmens, sodass Sie und die Server an Ihrem Arbeitsplatz auch dann bestens geschützt sind, wenn Sie unterwegs sind.

Wenn Sie viel auf Dienstreisen sind, wissen Sie nur zu gut, dass Sie manchmal auf einen öffentlichen WLAN-Hotspot angewiesen sind, da eine bestimmte Aufgabe nicht länger warten kann. Die Risiken öffentlicher WLANs zu kennen, reicht aber aus, damit Ihre wichtigen Geschäftsdaten nicht zur Beute von Hackern werden.

Weitere Artikel und Links zu öffentlichen WLANs

- Sicherheit für öffentliches Wi-Fi
- Schutz für Wi-Fi-Netzwerke
- Infografik: Sicherheit beim Online-Banking – So schützen Sie Ihr Geld
- Kaspersky Internet Security for Android
- Kaspersky Internet Security